AN INTRUDER IN YOUR POCKET: CITIZEN’S ARTIFICIAL INTELLIGENCE MONITORS USERS AND HIGHLIGHTS THE NECESSITY FOR EXPANDED INVASION OF PRIVACY TORTS

John W. Gillies

I. Introduction

As technology becomes more pervasive in our lives, the need to upgrade tort law to combat invasions of privacy by devices capable of listening to their human owners has never been more apparent. Now that the vast majority of the population has a smartphone in their pockets at all times, the privacy concerns are substantial, particularly with advancements in artificial intelligence (“AI”). The standard

1 See Robert D. Lang & Lenore E. Benessere, Alexa, Siri, Bixby, Google’s Assistant, and Cortana Testifying in Court, 89 N.Y. STATE BAR J. 8, 10 (2017) (commenting that “[v]oice control has rapidly evolved from a quirky and interesting technology, to a ‘must have’ capability in new devices.”). See also April White, A Brief History of Surveillance in America, SMITHSONIAN MAG. (Apr. 2018), archived at https://perma.cc/HL4X-6SVQ (questioning the future with electronic devices capable of listening). “Those smart speakers? They are essentially wiretaps. They are constantly listening. It’s a new type of corporate surveillance: If they listen to you, they can get you what you want, when you want. People like that. But where else will that data go?”

2 See Steven Feldstein & David Wong, New Technologies, New Problems – Troubling Surveillance Trends in America, JUST SEC. (Aug. 6, 2020), archived at https://perma.cc/UG7R-7QQ4 (analyzing the trends of increased surveillance with increasing use of artificial intelligence and considering how best to “maintain a positive balance between rights and law enforcement imperatives.”). See also Steven Feldstein, The Global Expansion of AI Surveillance, CARNEGIE ENDOWMENT FOR INT’L PEACE (Sept. 17, 2019), archived at https://perma.cc/8N9L-6PF2 (concluding that at least 75 out of 176 countries worldwide are actively using AI for the purpose of surveillance). “AI is not one specific technology. Instead, it is more accurate to
privacy concerns associated with technological advancements involve surveillance, like location services and personal data falling into the wrong hands. \(^3\) Smartphone application Citizen, which functions as a mix between a social media app and a police scanner, demonstrates the worst ways which a phone app can violate privacy laws.\(^4\) Citizen, when enabled, listens to users through an AI, and it is this feature where all these evolving technologies and issues converge.\(^5\)

Smartphones have given us instant messaging and constant news notifications; it only makes sense that an app would emerge to track and alert users of crime in real time.\(^6\) Citizen has localized and

---

think of AI as an integrated system that incorporates information acquisition objectives, logical reasoning principles, and self-correction capacities.” Id. See also Lang & Benessere, supra note 1, at 12 (detailing emerging privacy concerns, by stating that “[w]e are now at the start of an era in which previously unavailable data can be accessed, become discoverable and later be introduced into evidence.”).

\(^3\) See Feldstein, supra note 2 (noting that surveillance is not inherently unlawful, but also acknowledging that “intrusions profoundly affect an individual’s right to privacy” and these intrusions “may infringe upon an individual’s right to freedom of association and expression.”).

\(^4\) See Brian Heater, Controversial crime app Citizen launches $20/month Protect service, TECHCRUNCH (Aug. 3, 2021), archived at https://perma.cc/BQL7-SNYA (detailing the launch of Protect Mode, a feature in the app Citizen, which, “[w]hen enabled in a questionable situation, . . . will live monitor the user’s audio feed, using AI to detect for things like screams, offering up a connection to the agent. If you don’t respond, it will auto connect you.”); Brooke Auxier et al., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, PEWSCH.CTR. (Nov. 15, 2019), archived at https://perma.cc/UEQ7-UHXV (presenting the sentiment that 70% of adults think their data is less secure than it was five years ago); Feldstein & Wong, supra note 2 (noting that increased levels of surveillance are being seen worldwide).

\(^5\) See Sara Morrison, Citizen, the controversial safety app, is ready to profit from its fear-based platform, VOX (Aug. 3, 2021), archived at https://perma.cc/XV5J-A5TB (explaining the functionality of Protect Mode, which “comes with Distress Detection, where Citizen’s AI listens through its microphone for sounds of obvious distress (screaming) and then asks if they’d like to be connected to an agent (or automatically connects them if they don’t respond quickly)).”). See also Boone Ashworth, Citizen’s New Service Helps Paying Users Summon the Cops, WIRED (Aug. 3, 2021), archived at https://perma.cc/4JKL-V5NJ (explaining that Citizen’s new Protect Mode service has been “decried as overreaching” by privacy advocates).

\(^6\) See Abigail Weinberg, "It Creates a Culture of Fear": How Crime Tracking Apps Incite Unnecessary Panic, MOTHER JONES (Aug. 9, 2019), archived at https://perma.cc/GA3R-ABEY (noting that, “[w]hile the app purports to make communities safer, experts say that constant notifications about local crime, sent to thousands of city dwellers multiple times a day, can actually create a culture of fear.”).
personalized this stream of information, keeping users informed of every crime or dangerous occurrence, even those which they would have been otherwise unaware of. The steady stream of terrible news stokes fear and reinforces the user’s decision to continue to pay the monthly bill for the app, despite currently low crime rates in the U.S.

The concept behind Citizen was to create an app that tracks potentially dangerous incidents, opens up the 911 system to the general public, and notifies users when they are near incidents based on their smartphone location services. Citizen relies on input from human employees and AI technology which work in concert to generate and disperse information to users. Unfortunately, the app has proven to be less benevolent than the concept would suggest, as it was promptly removed from the Apple App Store shortly after its initial 2016 launch, under its original name “Vigilante,” for violating Apple’s App

---

7 See id. (detailing the dissonance between Citizen’s intent to make communities safer with the actual application of the technology, which sends out constant notifications to subscribers about local crime and serves to create a culture of fear).

8 See id. (explaining that Citizen presents unfiltered data “as if it’s authoritative, and it creates a culture of fear.”). Citizen is “designed to gamify paranoia and convince its users that their cities are dangerous places, that are in constant need of surveillance.” Id. The United States is in fact “experiencing one of the lowest crime rate periods in the country’s history.” Id.

9 See Lisa Summers & Keesha Johnson, First Crime Awareness App Launches in NYC Offering Real-Time Notifications and Live Broadcasting of Incidents, BUS. WIRE (Oct. 26, 2016), archived at https://perma.cc/3RHF-SAXB (quoting Vigilante CEO and Founder Andrew Frame, who stated within a press release: “[b]y using technology to access and open the 911 system, we can create transparency, eliminate bias, and unleash the most powerful, but yet untapped force in the fight against crime – citizens themselves.”). See also John Herrman, All the Crime, All the Time: How Citizen Works, N.Y. TIMES (Mar. 17, 2019), archived at https://perma.cc/CR5E-99LW (explaining how the Citizen app functions, and how the app developers hope it will be used).

10 See Heather Kelly, Citizen, the real-time crime alerting app, is growing in big cities, CNN BUS. (Mar. 12, 2019), archived at https://perma.cc/3Y7U-CQ68 (explaining generally the technology behind the app).

Using a combination of human employees and technology, Citizen scans hundreds of public-safety radio bands 24-hours a day in the major cities where it’s deployed, sometimes by playing audio at three times the speed. It filters out what it deems non-essential and sends the information as short, factual alerts to everyone within a quarter mile of the incident. The app updates with a list of details as they roll in and lets people nearby take live video or comment with information.

Id.
Developer Review Guidelines. Following the app’s brief stint on the App Store, the company reworked its image and settled on the new name Citizen, with the previous focus on possible intervention by users removed from the marketing materials.

Citizen was initially only a one-way notification system, but has since debuted new features, like Protect Mode and Distress Detection, which are part of Citizen’s effort to monetize their service.

---

11 See Sarah Perez, Controversial crime reporting app Vigilante banned from App Store, TECHCRUNCH (Nov. 2, 2016), archived at https://perma.cc/M4VH-Q3ZH (detailing Vigilante’s removal from the Apple App Store because the app encouraged and risked physical harm to users). See also Jack Crosbie, APPLE PULLS DANGEROUS ‘VIGILANTE’ APP FROM APP STORE, INVERSE (Oct. 29, 2016), archived at https://perma.cc/E9LY-EL8G (explaining further the circumstances that led to the removal of Vigilante from the Apple App Store). Citizen CEO Andrew Frame posted on his Facebook his thoughts behind Vigilante, writing:

“Through Vigilante we are exploring the relationship between transparency and justice. Can we use transparency to reduce crime? Can transparency be empowered responsibly through technology? What behavioral changes might this create? Are they good for the world? Can we use transparency to repair the relationship between community and police?” he writes. “We are hoping a long-term behavioral change will deter criminal behavior, and it will happen even faster in the areas where Vigilante has the best adoption.”

Id.

12 See Sarah Perez, Banned crime reporting app Vigilante returns as Citizen, says its ‘report incident’ feature will be pulled, TECHCRUNCH (Mar. 10, 2017), archived at https://perma.cc/XCH7-NN58 (listing off some of the changes made to the branding of the app, specifically the name and the addition of a pop up window offering “stronger guidance” to “never approach a crime scene, interfere with an incident, or get in the way of police[.]”).

13 See Morrison, supra note 5 (explaining the launch of Protect Mode and Distress Detection, two features launched on Citizen in August of 2021, which were available for a $20 monthly subscription). The subscription fee is Citizen’s first attempt at monetization. Id. Citizen has progressed from simply “alerting users to crimes, fires, and car accidents in their neighborhoods – to offer a service that protects users from or provides quick emergency services in response to those same types of incidents.”

Id.

Here’s how Protect works: Subscribers can either be directly connected to a Protect Agent by tapping Get Agent in their app, or they can swipe to enable Protect Mode. Protect Mode comes with Distress Detection, where Citizen’s AI listens through its microphone for sounds of obvious distress (screaming) and then asks if they’d like to be connected to an agent (or automatically connects them if they don’t respond quickly); or they can use the “Shake for Agent” option, where they’re discreetly connected to
Even with the new image and name, Citizen has been condemned by experts for multiple reasons, including fostering an outlet for racism, allowing the app’s COVID-19 tracking data to be breached, and creating privacy concerns based on the audio surveillance nature of the Protect Mode feature.\(^\text{14}\) The criticism also extends to Citizen’s CEO Andrew Frame, who in addition to other scandals, used the app to place a bounty on a man who was entirely innocent of the accused crime of starting a wildfire, offering up $30,000 for information on this man who was cleared by police before the mob was able to locate him.\(^\text{15}\)


\(^\text{15}\) See Joseph Cox & Jason Koebler, ‘FIND THIS FUCK:’ Inside Citizen’s Dangerous Effort to Cash In On Vigilantism, VICE (May 27, 2021), archived at https://perma.cc/Q64Q-URSV (explaining a May 2021 scandal in the Los Angeles, California area where Citizen Founder and CEO Andrew Frame issued a bounty on a man Citizen suspected to have started a wildfire, who was later determined to be entirely innocent). The bounty notice was broadcast to the 848,816 citizen users in the Los Angeles area, with the price for information rising as high as $30,000, before the app rescinded the bounty when it became clear the man had no relation to the fires. Id. See also Sara Ashley O’Brien, Citizen says it’s not starting its own private
Citizen had previously been pursuing a working relationship with the Los Angeles Police Department, who cut ties with the app shortly after the botched manhunt.\textsuperscript{16} This has not deterred the leadership group at Citizen, whose latest expansion ideas include an on-demand security service for Citizen users in Chicago, as well as implementing access for Ukrainians during the ongoing attack from Russia.\textsuperscript{17}

This note will focus on personal privacy issues presented by Citizen Protect Mode, as well as AI surveillance concerns, whether AI can violate privacy laws, and will also include a proposal for an increase in the strength of the invasion of privacy torts. AI, as a new and evolving field, has yet to be fully legislated and regulated.\textsuperscript{18}

\textit{security force -- but it won’t rule out hiring someone else to do it, CNN Bus. (May 27, 2021), archived at https://perma.cc/ZK3D-U8Z8} (detailing a “personal rapid response service,” which “sparked questions and concerns about the potential use cases and pitfalls of on-demand privatized security.”). A Citizen spokesperson addressed the concerns and stated that the company has “no plans to launch our own private security force.” \textit{Id.}

\textit{See Joseph Cox, LAPD Emails Reveal Fallout of Citizen’s Botched Manhunt, VICE (Jan. 27, 2022), archived at https://perma.cc/966S-AYQC} (recounting the decision of the LAPD to end talks with Citizen, based on “serious concerns with Citizen, and the user actions they promote and condone[.]”).

\textit{See Adi Robertson, Citizen reportedly plans to test a private security partnership in Chicago, THE VERGE (Mar. 21, 2022), archived at https://perma.cc/8QEY-LB5D} (detailing Citizen leadership’s plans to partner with private security company Securitas in Chicago to test a private security feature for their application). The partnership would “function as a check-in service’ for users.” \textit{Id. “Securitas could follow up after someone reported a break-in to make sure they’re all right[.]”} \textit{Id. See also Joseph Cox, Citizen Planning to Trial On-Demand Private Security in Chicago, VICE (Mar. 21, 2022), archived at https://perma.cc/XQ4J-QPVV} (noting the differences between the LA trial and this Chicago trial program). “[The Los Angeles] trial differed slightly from the planned Chicago one, in that it was designed for private security to rapidly respond to someone in danger and evacuate them to safety, rather than perform check-ins or arrive at a previously scheduled time.” \textit{Id. See also Joseph Cox, Neighborhood Crime App Citizen Is Trying to Expand to Ukraine, VICE (Mar. 11, 2022), archived at https://perma.cc/5SJF-A6XN} (explaining Citizen’s ambition to expand into Ukraine, to help keep the people aware of incidents and areas to avoid). Citizen’s plan for expanding to Ukraine involved a partnership with CBS, who would provide footage, which Citizen would then disseminate to the app users. \textit{Id. The proposed partnership between Citizen and CBS did not materialize even after the two sides met for discussions. Id.}

\textit{See Bradford K. Newman, Recent Developments in Artificial Intelligence Cases 2021, A.B.A. (June 16, 2021), archived at https://perma.cc/MR6D-A49E} (listing recent cases involving AI and noting that “[b]efore any substantive federal legislation is enacted, many legal issues related to AI will play out in state and federal courts around the country.”).
audio heard through the user’s phone is monitored by an AI, which, when triggered, connects the user to a Citizen employee (“Agent”) who can offer assistance and contact law enforcement. While the Citizen subscriber can consent to monitoring by AI and an Agent if there is a detection of distress, any third party who is monitored by Citizen would have no opportunity to consent. This surveillance concern multiplies when the Citizen user enables Protect Mode as a guest in another’s home, where the homeowner has a subjective expectation of privacy that society recognizes as reasonable. Citizen has tremendous promise as a protection tool, but the expanding nature of the app means either that the AI technology used for surveillance must be legislated to ensure compliance with state recording statutes, or invasion of privacy torts must be drastically expanded to provide a legitimate recourse for individuals who feel their privacy rights have been violated.

19 See Binder, supra note 13 (reporting a statement from a Citizen spokesperson concerning privacy concerns surrounding the AI recording feature). A Citizen spokesperson asserted that while AI-technology is monitoring the audio from the phone, “no human is ever listening to a user’s audio.” Id. The Citizen spokesperson acknowledged that there is data recorded (such as protection data) from the Distress Detection, which is deleted after 30 days. Id. See Heater, supra note 4 (noting that Citizen Agents “can escalate to 911, provide first responders with your precise location . . . or simply stay connected with you and monitor you until you feel safe again.”). A job listing for a Citizen Protect Agent read:

In this role, you will be communicating with users who are in need of assistance in potentially unsafe conditions. You will be responsible for guiding difficult conversations and using your best judgement in determining the severity of these situations in real-time. You will be at the frontlines of helping users who feel unsafe in their surroundings and offer direct assistance and escalation to 911.

Id.

20 See Binder, supra note 13 (discussing a concern relating to Citizen Protect mode, where a “customer may consent to Distress Detection, [but] a nearby non-customer third-party could surely have concerns about the service spying or snooping on them.”). See Heater, supra note 4 (detailing how the app live monitors the user’s audio feed, with no mention of third-party consent). Citizen Protect Mode “offers quick access to [an] agent. When enabled in a questionable situation, the app will live monitor the user’s audio feed, using AI to detect for things like screams, offering up a connection to the agent.” Id.
II. History

A. The Fourth Amendment and Privacy from the Government

The Constitution protects a right to privacy from state actors through the Fourth Amendment, and the Supreme Court has held “that searches and seizures inside a home without a warrant are presumptively unreasonable.” The Fourth Amendment offers protections from searches and seizures in situations where the individual exhibits a subjective expectation of privacy that society recognizes as reasonable. A subjectively reasonable expectation of privacy exists if the individual takes measures to ensure privacy in their location. The home has the highest protections for privacy, but a subjectively reasonable expectation of privacy can even be extended.

21 See U.S. Const. amend. IV (detailing the individual’s right to privacy). The Fourth Amendment reads:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.


22 See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing the two-prong requirement for privacy rights). First, a person must exhibit an actual (subjective) expectation of privacy, and second, that expectation of privacy must be one that society recognizes as reasonable. Id.

23 See id. at 360 (determining “that an enclosed telephone booth is an area where, like a home . . . a person has a constitutionally protected reasonable expectation of privacy.”); Olmstead v. United States, 277 U.S. 438, 474–75 (1928) (Brandeis, J., dissenting) (summarizing the Fourth Amendment right to privacy by saying, “[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited . . . .”); Benjamin Zhu, A Traditional Tort For A Modern Threat: Applying Intrusion Upon Seclusion To Dataveillance Observations, 89 N.Y.U. L. REV. 2381, 2405 (2014) (explaining that “the Fourth Amendment follows the secrecy paradigm and generally does not protect activities in the public sphere.”).
to a closed phone booth. The expectation of privacy is waived if the person exposes private affairs to the world. Privacy can even be unintentionally waived in one’s own home if actions are exposed to the outside world through excessive volume or an open window.

Privacy rights are strongest in the home, with only limited circumstances where a warrantless search of the home is reasonable. Under the doctrine of exigent circumstances, police can search without a warrant in emergency circumstances, provided there is probable cause. Exigent circumstances include when police: in hot pursuit of a felon, are protecting someone who is in danger, or need to prevent

24 See Katz, 389 U.S. at 361 (explaining that a closed phone booth carries with it a subjective expectation of privacy that society recognizes as reasonable, because the defendant tried to withhold the conversation from the public).
25 See id. (stating that “a man’s home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited.”). Therefore, an unreasonable expectation of privacy is when one expects conversations in the open to be protected from being overheard. Id.
26 See id. at 351 (articulating how “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”). “[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” Id.
27 See Daniel T. Pesciotta, I’m Not Dead Yet: Katz, Jones, And The Fourth Amendment In The 21st Century, 63 CASE W. RES. L. REV. 187, 215 (2012) (stating that “the Court has always been steadfast in its protection of privacy in the home—an area in which all citizens undoubtedly expect the utmost level of privacy.”).
28 See John Mark Huff, Warrantless Entries And Searches Under Exigent Circumstances: Why Are They Justified And What Types Of Circumstances Are Considered Exigent?, 87 U. DET. MERCY L. REV. 373, 380 (2010) (listing the three scenarios where exigent circumstances can be present: “hot pursuit, destruction of evidence, and protection of police/public.”). “Exigent circumstances are situations where ‘real immediate and serious consequences’ will ‘certainly occur’ if a police officer postpones action to obtain a warrant.” Id.
the destruction of evidence. Absent exigent circumstances, there is “a firm line at the entrance of the house” for search purposes.

The Fourth Amendment’s protections have been considered extensively, but there is still limited case law on more “modern” technology. The Fourth Amendment’s applicability in cases involving advanced technology has yet to be fully determined, but often hinges on the availability of the technology to the public.

29 See Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 298–99 (1967) (explaining the circumstances that would satisfy the hot pursuit standard by stating that “The Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others.”); Brigham City, Utah v. Stuart, 547 U.S. 398, 400 (2006) (noting that police may enter a home without a warrant when they have an objectively reasonable basis for believing that an occupant is seriously injured or imminently threatened with such injury); Kentucky v. King, 563 U.S. 452, 472 (2011) (holding that the suspected sound of destruction of evidence was a sufficient exigent circumstance, because the police did not create the exigent circumstance).

30 See Payton v. New York, 445 U.S. 573, 590 (1980) (noting that “the Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.”). “The zealous and frequent repetition of the adage that a ‘man’s house is his castle,’ made it abundantly clear that both in England and in the Colonies, ‘the freedom of one’s house’ was one of the most vital elements of English liberty.” Id. at 596–97.

31 See Pesciotta, supra note 27, at 240 (detailing generally the lack of case law dealing with what would be considered more modern technology). There is concern among commentators, who “have expressed concern as to whether the reasonable expectation of privacy test developed in Katz will continue to adequately protect citizens’ Fourth Amendment rights in this age of ever-advancing technology.” Id. at 189. “Many rapidly advancing technologies with serious Fourth Amendment implications, such as video surveillance, have yet to come before the Court in any Fourth Amendment context.” Id. at 215. “[T]he Court has never ruled on a Fourth Amendment case dealing with a search of information on the internet.” Id. at 215.

But see id. at 191 (explaining concerns over privacy protections).

While there is concern that privacy protections will be reduced in this technological age, “in the only two Fourth Amendment and technology cases the Court has heard during this century, Kyllo and Jones, the Court ruled in favor of the defendant and thus actually served to protect citizens’ privacy—not erode it.” Id. The cases decided post-Katz “do not indicate that the reasonable expectation of privacy test developed in Katz is unable to protect citizens’ Fourth Amendment rights from modern technology.” Id. at 201.

32 See Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imaging device by the police from the outside street to detect heat within a private home violates one’s reasonable expectation of privacy, partially because the technology was not publicly available); United States v. Jones, 565 U.S. 400, 404–05 (2012) (holding that by attaching a GPS tracking device to an individual’s vehicle
Fourth Amendment’s prohibition on unreasonable searches and seizures has been tested even further in *Carpenter v. United States*, where the Supreme Court held the use of a defendant’s cell phone records was an unreasonable search.\(^{33}\)

**B. The Right to Privacy from Private Companies—The Tort of Invasion of Privacy**

1. *The Right to Privacy* by Samuel Warren and Louis Brandeis

While the Fourth Amendment addresses privacy concerns, it is only controlling when the violation is performed by a government actor.\(^{34}\) The first publication in the U.S. to advocate for a right to privacy in tort law was written by Samuel Warren and Louis Brandeis in 1890, and continues to be the most influential publication on the topic to this day.\(^{35}\) That article, *The Right to Privacy*, describes that and then using the GPS to track the vehicle’s movements on public streets, the government violated the defendant’s property rights. *See also* Pesciotta, *supra* note 27, at 209 (articulating that in Kyllo, the Supreme Court made clear that the need to ensure citizens’ rights in the face of advancing technology was paramount).

\(^{33}\) *See* Carpenter v. United States, 138 S.Ct. 2206, 2223 (2018) (declining “to grant the state unrestricted access to a wireless carrier’s database of physical information.”). The Supreme Court’s holding in *Carpenter* stated that “the deeply revealing nature of CSLI [“cell-site location information”], its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.” *Id.* *See also* Elizabeth E. Joh, *Artificial Intelligence and Policing: Hints in the Carpenter Decision*, 16 OHIO ST. J. CRIM. L. 281, 290 (2018) (detailing the Court’s thought process in the Carpenter case, which suggests a concern about the type of investigation techniques utilized, describing them as “superhuman, passive, and automated.”).

\(^{34}\) *See* Benjamin E. Bratman, *Brandeis And Warren’s “The Right To Privacy And The Birth Of The Right To Privacy”*, 69 TENN. L. REV. 623, 634 (2002) (acknowledging the Fourth Amendment’s protections are limited to instances of privacy invasions from state actions).

\(^{35}\) *See id.* at 626 (noting that judges and scholars continue to cite to this law review article “as the original source of a right to privacy in American legal history.”). The historical significance of the article in the formation of privacy law cannot be overstated, as “[t]he law and the legal and historical literature from the late nineteenth century and early twentieth century strongly support the argument that Brandeis and Warren’s article did indeed ‘give birth’ to a right to privacy.” *Id.* The article presented “the need for the common law to respond to society’s new threats to privacy by giving privacy its own legal protection.” *Id.* at 650. Brandeis and
right as “the right to be let alone.” In *The Right to Privacy*, Warren and Brandeis created the four invasion of privacy torts laid out in the Restatement (Second) of Torts, which are recognized in the majority of American jurisdictions today. The creation of these four invasion of privacy torts grew out of an inadequacy of nineteenth century privacy protections. Warren and Brandeis acknowledged the Fourth

Warren “should not be denied their place as the inventors of the right to privacy, and their article should not be denied its status as a true classic in legal literature.” *Id.* at 651.

36 See Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, HARV. L. REV. 193, 193 (1890) (explaining generally how the principle “[that] the individual shall have full protection in person and in property” has expanded and evolved to create remedies encompassing not only physical interference, but also “man’s spiritual nature . . . and his intellect” and eventually “the right to be let alone.”); Bratman, *supra* note 34, at 627 (summarizing Warren and Brandeis’s article, explaining that “the premise of their legal argument was that the law should recognize a general right ‘to be let alone.’”). *See* Warren & Brandeis, *supra* note 36, at 193 (expanding on the right to be let alone by adding “the right to liberty secures the exercise of extensive civil privileges; and the term ‘property’ has grown to comprise every form of possession – intangible, as well as tangible.”).

37 See *Id.* at 624 (listing the four invasion of privacy torts which have their origins in *The Right to Privacy*). “(1) ‘unreasonable intrusion upon the seclusion of another,’ (2) ‘appropriation of the other’s name or likeness,’ (3) ‘unreasonable publicity given to the other’s private life,’ and (4) ‘publicity that unreasonably places the other in a false light before the public.’” *Id.* “Brandeis and Warren’s work is almost universally regarded as the origin of the four invasion of privacy torts that are recognized in most American jurisdictions today and that are laid out in the Restatement (Second) of Torts. . . .” *Id.* at 624.

38 See *id.* at 632–33 (recounting nineteenth century privacy protections, which were limited to: libel, the Fourth Amendment, the tort of trespass, criminal eavesdropping laws, and injunctions preventing publication of private letters). “[E]xcepting protections provided through the criminal law, such as the Fourth Amendment or statutes making eavesdropping a crime, purported protections of privacy in nineteenth century American legislation and common law were merely by-products of equitable and legal remedies designed to address other wrongs.” *Id.* at 632–33. *See also* Warren and Brandeis, *supra* note 36, at 196 (explaining that as society advances, so must the law to protect individual privacy).

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

*Id.*
Amendment as “a source of significant protection for personal privacy,” but noted its major limitation: it only covers state action and is useful to aggrieved parties only when the invasion of privacy was by state actors.\(^{39}\)

2. Privacy by William Prosser

Brandeis and Warren wrote *The Right to Privacy* in response to issues they had with journalists of their day prying into people’s private lives and publishing what they found, but this right to privacy has extended into new technologies and evolved to encompass a more general right to privacy than that of an overzealous press.\(^{40}\) The invasion of privacy torts may have their origin in *The Right to Privacy*, but it was later in the twentieth century when William Prosser gave the torts a new order and legitimacy by systemizing Brandeis and Warren’s work in his own law review article, *Privacy*.\(^{41}\) Prosser organized the invasion of privacy into four distinct torts:

\(^{39}\) See Bratman, *supra* note 34, at 634 (explaining that the Fourth Amendment only applies to invasions of privacy from state action). “[W]hile a source of significant protection for personal privacy, the Fourth Amendment to this day covers only state action and safeguards against just certain types of intrusions on privacy. Hence, it was not helpful toaggrieved parties, except in a small category of cases.” *Id.* at 633. *See also* Jason Owens, *Hearing Thy Neighbor: The Doctrine of Attenuation and Illegal Eavesdropping by Private Citizens*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 177, 178 (2007) (asserting the complications that arise “[w]hen police receive tips based on a private citizen’s illegal eavesdropping, follow-up investigations are difficult because the rule of exclusion calls for the suppression of evidence ‘derived from’ the underlying illegal eavesdropping.”).

\(^{40}\) See Scott Jon Shagin, *The Prosser Privacy Torts In A Digital Age*, N.J. LAW. MAG., Apr. 2008, at 9 (detailing how *The Right to Privacy* “famously spawned a body of law termed ‘the right to privacy’ which evolved . . . for half a century” and created a legacy of privacy torts which “are increasingly implicated in the use and misuse of technology in a digital world.”). The Prosser Privacy Torts are applicable even today, because “technology-enabled newsgathering techniques and digital intrusion [are] growth industries, [thus] there has never been a greater need to understand the metes and bounds of the Prosser privacy torts.” *Id.* at 10.

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.

Prosser’s torts, as the leading torts scholar of his time, were readily embraced by the courts. The legacy of Prosser’s torts is substantial; nearly all states recognize, in either common law or statute, at least one form of his synthesized privacy torts. However, these tort laws have not emerged as the leading protector of privacy that Prosser had hoped.


See Prosser, supra note 41, at 389 (listing the four invasion of privacy torts synthesized by Prosser). In crafting the tort of intrusion, Prosser determined “that the interest protected by this branch of the tort is primarily a mental one. It has been useful chiefly to fill in the gaps left by trespass, nuisance, the intentional infliction of mental distress . . . .” Id. at 392. Prosser noted that his second tort, the public disclosure of private facts, “is in reality an extension of defamation, into the field of publications that do not fall within the narrow limits of the old torts, with the elimination of the defense of truth.” Id. at 398. Prosser’s third tort, false light in the public eye, protects reputation, “with the same overtones of mental distress as in defamation.” Id. at 400. In discussing his fourth privacy tort, appropriation, Prosser notes that “[t]he interest protected is not so much a mental as a proprietary one, in the exclusive use of the plaintiff’s name and likeness as an aspect of his identity.” Id. at 406.

See Richards & Solove, supra note 41, at 1890 (expounding Prosser’s reputation during his lifetime and the court’s willingness to adopt his articulated invasion of privacy torts). “As the leading torts scholar of his time, Prosser was able to ensure that his interpretation of the privacy torts became the dominant one.” Id.

See id. (describing the legacy of the Prosser privacy torts and their nearly universal recognition nationwide). But see id. (noting that while Prosser’s contribution to privacy torts was substantial, “he also stunted its development in ways that have limited its ability to adapt to the problems of the Information Age.”). Prosser’s rigid categorization of privacy torts into four categories “stripped privacy law of any guiding concept to shape its future development. Prosser thus greatly increased tort privacy’s stature at the cost of making it harder for privacy law to adapt to new circumstances in the future.” Id.
they would.\textsuperscript{45} When examining invasion of privacy concerns from the media, these Prosser torts have not provided the level of protection originally sought in \textit{The Right to Privacy}.\textsuperscript{46} Additionally, invasion of privacy tort laws have not been effectively adapted to more modern problems like the extensive collection of data and personal information by businesses.\textsuperscript{47}

Of the four invasion of privacy torts, the tort of intrusion is the one most likely to lead to regulation for the collection of information.\textsuperscript{48}

\textsuperscript{45} See id. at 1918 (stating that “tort law has not emerged as the leading protector of privacy.”). “If privacy law were a stock, its performance over the last century would not be deemed impressive. It has been a consistently poor achiever, barely keeping up with inflation.” Richards & Solove, supra note 41, at 1918. “Today, the chorus of opinion is that the tort law of privacy has been ineffective, particularly in remedying the burgeoning collection, use, and dissemination of personal information in the Information Age.” Id. at 1889. See also Danielle Keats Citron, \textit{Mainstreaming Privacy Torts}, 98 CAL. L. REV. 1805, 1805 (2010) (summarizing the issues Prosser’s privacy torts have had with adjusting to modern technology). “[C]ourts have too often rigidly interpreted the four privacy torts. Prosser’s conceptualization of privacy interests worth protecting is too narrow to accommodate the privacy interests implicated by networked technologies. As a result, the privacy torts often cannot properly redress contemporary privacy injuries.” Id. at 1806. See also McClurg, \textit{Bringing Privacy Law Out of the Closet}, supra note 41, at 991–92 (reflecting that “tort law currently provides little protection from intrusive videotaping, photography, or surveillance, so long as the activity occurs in a public place.”); Shagin, supra note 40, at 9 (noting that “it is tempting to conclude that the Prosser privacy torts have continued to evolve . . . [b]ut, in fact, the privacy torts have evolved unevenly.”).

\textsuperscript{46} See Richards & Solove, supra note 41, at 1918–19 (detailing the limited effect invasion of privacy torts have had on protecting individuals from invasions by the media). See also Bratman, supra note 34, at 624 (detailing the motivation behind Brandeis and Warren’s article, which was to “[chastise] the journalists of their day, particularly photojournalists, for prying into people’s private lives in search of tawdry and alluring ‘news’. . . .”).

\textsuperscript{47} See Richards & Solove, supra note 41, at 1918 (pointing out the privacy torts’ inability to adapt to modern privacy problems surrounding data collection by private businesses). See also Citron, supra note 45, at 1805 (stating that “privacy tort law is ill-equipped to address these changes.”). “Although Prosser’s privacy taxonomy tackled privacy injuries caused by twentieth-century technologies, it may not be dynamic enough to address privacy injuries produced by digital networks.” Id. at 1809. The right to privacy is implicated by contemporary problems like revealing personal information to inadvertently endanger oneself to potential assailants. Id. at 1833.

\textsuperscript{48} See Richards & Solove, supra note 41, at 1919 (noting that the tort of intrusion is the most likely to combat information collection, but that data compilation occurs from public domain information, which courts have ruled “is not an invasion into a person’s ‘solitude’ or ‘seclusion.’”).
The justification for making the observation of personal information its own distinct tort stems from a societal interest in helping individuals protect their “dignity, autonomy, and self-determinism.” Intrusion of privacy, as Prosser formulated, applies to surreptitious surveillance and other nonphysical invasions of privacy. For example, the tort of intrusion has been applied by courts in cases of eavesdropping through wiretapping and microphones, as well as interceptions of private phone calls. Prosser’s invasion of privacy by intrusion deals with the type of privacy “invaded by physical intrusion upon the plaintiff’s seclusion or solitude, or his private affairs,” which is why it is most suited to address surveillance of those who have not consented.

49 See Jane Y. Bambauer, The New Intrusion, 88 NOTRE DAME L. REV. 205, 213 (2012) (noting that “[p]rivacy scholarship promotes the use of law to protect interests in dignity, autonomy, and self-determinism.”). See also Zhu, supra note 23, at 2402 (stating that protecting individuals from invasions of privacy must apply to “unwanted observation[s] of one’s personal information . . . whether it occurs through traditional methods of surveillance or through the modern method of dataaveillance.” Id. “[T]he intrusion tort should recognize that dataaveillance’s observation of new personal information, unknown and unknowable from the individual pieces of data, constitutes a separate privacy intrusion, distinct from the intrusion occurring at the data collection stage.” Id.

50 See Zhu, supra note 23, at 2402–03 (summarizing Prosser’s tort of intrusion). The intrusion tort, Prosser noted, “had been applied to ‘eavesdropping upon private conversations’ through the use of wiretapping and microphones and to ‘peering into the windows of a home.’” Id. at 2403.

51 See id. (listing some general scenarios where the intrusion tort has been accepted by the courts, which serve to demonstrate “that the intrusion tort can apply to surveillances even absent some trespass-related misconduct and even if the victim is initially unaware of the surveillance.”). The court has even recently “allowed intrusion claims based on the interception of private phone calls, secret videotaping of private matters, unauthorized inspection of personal credit history, and unconsented examination of credit card records, even when the records were lawfully within the defendant’s possession.” Id.

52 See J. THOMAS MCCARTHY & ROGER E. ScheonTER, THE RIGHTS OF PUBLICITY AND PRIVACY § 1:20, Prosser’s four torts of privacy – Prosser’s first tort: invasion of privacy by intrusion (2d ed. 2021) (detailing the specific variety of privacy that is protected by this tort). Peeping toms, eavesdroppers, and wiretappers make up this category. Id.

What Prosser called invasion of privacy by intrusion is probably the type of privacy envisioned within the 1948 United Nations Universal Declaration of Human Rights: ‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, not to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.’
3. Present Data Privacy Tort Laws

Tort actions for data privacy violations are not particularly practical, based on limitations built into tort law itself.\(^{53}\) While tort laws on the books for invasion of privacy are largely ineffective, the advantage of attacking this issue with tort actions is attractive when compared to enacting sweeping legislation.\(^{54}\) Privacy tort law has over a century of history behind it, and the biggest hurdle is simply adapting it to address the privacy problems with big tech and big data.\(^{55}\)

The privacy tort most likely to address Protect Mode is the intrusion upon seclusion.\(^{56}\) The intrusion tort is most related to the tort of trespass, and “has been used chiefly to fill the gaps left by trespass.”\(^{57}\) Intrusion Upon Seclusion, as explained in the Restatement (Second) of Torts, does not depend on the publicity given to the person

\(^{53}\) See Andrew J. McClurg, A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 NW. U. L. REV. 63, 97 (2003) (suggesting a tort response for protecting information privacy and noting the “view that current tort law simply is not well suited to address information privacy abuses.”).

\(^{54}\) See id. (explaining the advantage tort law has for addressing data privacy concerns, specifically that “because it would not require enabling legislation, tort law is the only solution that presents a feasible current option.”).

\(^{55}\) See id. at 98 (detailing the sort of regulatory system that already exists in tort law, while admitting “that the development of privacy tort law has not been a model of efficiency, privacy tort law does have the benefit of a century of experience behind it.”).

\(^{56}\) See Eli A. Meltz, No Harm, No Foul? “Attempted” Invasion of Privacy and the Tort of Intrusion Upon Seclusion, 83 FORDHAM L. REV. 3431, 3439 (2015) (quoting from section 652B of the Restatement (Second) of Torts, which states that “[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”); RESTATEMENT (SECOND) OF TORTS: INTRUSION UPON SECLUSION § 652B (1977) (outlining the elements of the Intrusion upon Seclusion tort). See also Bambauer, supra note 49, at 275 (explaining the basics of the tort of intrusion upon seclusion, noting that “the intrusion tort imposes liability for obnoxious observations.”). “Intrusion offers a principled way to penalize space invaders without unduly taxing the benefits society enjoys from open information exchange.” Id.

\(^{57}\) See Meltz, supra note 56, at 3452 (explaining the place in tort law occupied by intrusion in the invasion of privacy torts).
who was invaded, but rather relies on an intentional interference with another’s “interest in solitude or seclusion.”

An action for intrusion upon seclusion has varying viability depending on the court, as some require the defendant to observe or overhear the plaintiff. In states that don’t require the defendant to have observed or overheard the plaintiff, an action for Intrusion Upon Seclusion exists if a recording device has simply been placed or installed. The most important case on this principle is *Hamberger v. Eastman*, which held that a landlord simply placing a listening and recording device in his tenant’s bedroom without the tenant’s consent or knowledge was an invasion of privacy. Conversely, there are


The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.

**Id.**

59 *See* Meltz, *supra* note 56, at 3454 (describing the conflicting decisions between state courts as to “whether proof of observation or acquisition of information about the plaintiff is a necessary component of an intrusion upon seclusion claim.”). There are cases which support the conclusion “that an intrusion can occur when the plaintiff is not viewed or observed,” as well as “cases that have taken the opposite approach.” *Id. See also* Zhu, *supra* note 23, at 2403 (explaining that “[t]he viability of intrusion upon seclusion . . . demonstrates that the intrusion tort can apply to surveillances even absent some trespass-related misconduct and even if the victim is initially unaware of the surveillance.”).

60 *See* Meltz, *supra* note 56, at 3454 (generalizing a selection of cases which generally held that “a cause of action for intrusion upon seclusion exists even if the defendant has not viewed, recorded, heard, or otherwise observed the plaintiff – that is, the placement of a recording device alone is sufficient.”). *See also* Harkey v. Abate, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (holding that the installation of a hidden viewing device “can itself constitute a sufficient wrongful intrusion into the seclusion of a plaintiff . . . so as to permit recovery.”); Amati v. City of Woodstock, Ill., 829 F. Supp. 998, 1010–11 (N.D. Ill. 1993) (determining that “[t]he placing of a recording device in an area where one has a reasonable expectation of privacy is both intrusive and disruptive . . . the lack of allegations that anyone actually listened to the recorded telephone conversations do not defeat plaintiffs’ claims.”); Kohler v. City of Wapakoneta, 381 F. Supp. 2d 692, 704 (N.D. Ohio 2005) (holding that simply placing a device is sufficient for Intrusion Upon Seclusion).

61 *See* Hamberger v. Eastman, 206 A.2d 239, 242 (N.H. 1964) (articulating that court’s interpretation of the tort of Intrusion Upon Seclusion). “The tort of intrusion on the plaintiffs’ solitude or seclusion does not require publicity and communication
courts which do require proof that the defendant actually observed the plaintiff. 62

C. History of Electronic Surveillance


Within the Omnibus Crime Control and Safe Street Act of 1968 is Title III, which governs conduct used “to intercept audio, video, or electronic communications.” Title III does allow recordings with only one-party consent, and also bans the manufacture, sale, and possession of devices like eavesdropping equipment which could be

to third persons although this would affect the amount of damages . . . . ” Id. “For the purposes of the present case it is sufficient to hold that the invasion of the plaintiffs’ solitude or seclusion, as alleged in the pleadings, was a violation of their right of privacy and constituted a tort for which the plaintiffs may recover damages to the extent that they can prove them.” Id.

62 See Meltz, supra note 56, at 3458 (describing generally a collection of cases which “require the plaintiff to show that the defendant recorded, heard, viewed, or otherwise observed the plaintiff to constitute an intrusion upon seclusion.”). See also Meche v. Wal-Mart Stores, Inc., 692 So.2d 544, 550 (La. Ct. App. 1997) (determining that the installation of a bathroom camera at a Wal-Mart was not sufficient on its own for an intrusion upon seclusion, because “there is no evidence that any viewing of personnel took place or that any tapes were made of anyone in the restroom.”); LeCrone v. Ohio Bell Tel. Co., 201 N.E.2d 533, 537–38 (Ohio Ct. App. 1963) (noting that the presence of a phone tap was not sufficient, because the “defendant did not in fact intercept any conversations.”); Johnson v. Allen, 613 S.E.2d 657, 660 (Ga. Ct. App. 2005) (explaining that the defining issue in this case was not whether the device was installed, but whether the defendant had actively used it to monitor the women’s restroom).


[T]he Federal Wiretapping Act §§ 2510-2521, generally governs the conduct employed to intercept audio, video, or electronic communications. As stated, the Wiretap Act allows for recordings to be made with one-party consent, but 18 U.S.C. § 2512 creates a tension in the law by explicitly outlawing the possession and use of certain types of audio, video, or electronic equipment that individuals may utilize to record conversations that attorneys would otherwise have thought legal to use.

Id. at 24–25.
worn by a party to a conversation, based on a primary use analysis.\textsuperscript{64} Rather than give an exhaustive list of prohibited technology, Title III applications in court rely on interpretations of key phrases in the statute by focusing on the design of the recording equipment and whether the primary use of the product is for surreptitious recording.\textsuperscript{65} In addition to prohibitions on recordings and recording equipment, Title III granted civil remedies, including money damages and equitable relief, to individuals victimized by people who use these prohibited devices.\textsuperscript{66}

2. Electronic Communications Privacy Act of 1986

Before internet access and smartphones, the Electronic Communications Privacy Act of 1986 ("ECPA") was passed, establishing standards for law enforcement access to electronic records stored on remote servers.\textsuperscript{67} The ECPA updated the Federal Wiretap

\textsuperscript{64} See Federal Wiretapping Act, 18 U.S.C. § 2511 (1968) (allowing for recordings with only one-party consent, which need only be furnished by the person making the recording). See id. at § 2512 (banning the manufacture, sale, and possession of devices that could be used for eavesdropping). See also United States v. Spy Factory, Inc., 951 F. Supp. 450, 469 (S.D.N.Y. 1997) (illustrating the “primary use” determination of a surreptitious recording device, “emphasiz[ing] the objective determination of a device’s most probable use. This objective standard is substituted for the more individualistic and thereby problematic determination of what the device’s ‘primary’ use to any one consumer might be.”).

\textsuperscript{65} See Goldberg, supra note 63, at 25 (detailing the process that the courts use for determining whether a specific device is prohibited or not). “§ 2512 simply states that ‘[t]he statutory phrase is intended to establish a relatively narrow category of devices whose principal use is likely to be for wiretapping and eavesdropping.’” Id. See also United States v. Spy Factory, Inc., 951 F. Supp. at 471 (recounting the court’s decision to treat surreptitious with the plain meaning of the term: “secret or clandestine.”).

\textsuperscript{66} See Goldberg, supra note 63, at 25 (summarizing the civil remedies for victims found in 18 U.S.C. § 2520). In addition to money damages and equitable relief, civil remedies can also include “money damages in the form of compensatory and punitive damages.” Id. “[I]t is entirely possible for a person to be federally prosecuted for intentionally possessing a device that falls under the ambit of 18 U.S.C. § 2512 even if the person did not violate local law . . . .” Id.

\textsuperscript{67} See Deirdre K. Mulligan, Reasonable Expectations In Electronic Communications: A Critical Perspective On The Electronic Communications Privacy Act, 72 GEO WASH. L. REV. 1557, 1557 (2004) (explaining broadly the purpose and impact of the ECPA in a time when internet access was generally limited to the business community). “[The ECPA] created the statutory framework of privacy protections and related standards for law enforcement access covering electronic communications and remotely stored electronic records.” Id.
Act of 1968, which only addressed communication through “hard” telephone lines. This update applied to digital and electronic communications. Multiple privacy concerns motivated the act: (1) multiple copies are created when sending an email, which can be accessed after sending by non-parties to the communication, and (2) the practical difference of sending an email with multiple copies meant there was a potential for Fourth Amendment privacy violations.

Congress has known for decades that technology and telecommunications are continually progressing beyond existing privacy protections applied to communication technology. The ECPA modified the Federal Wiretap Act of 1968, which was passed before the invention of electronic communications. Title III focused on “aural acquisition” of voice communications. For the ECPA,

68 See Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510–2523 (2022) (updating the protections for conversations made through electronic equipment, which had previously only included telephone lines). Generally, “[t]he ECPA . . . protects wire, oral, and electronic communications whole those communications are being made, are in transit, and when they are stored on computers.” Id.

69 See id. (explaining the purpose behind the ECPA, which extended privacy protections to computer and other digital communications). See also, Mulligan, supra note 67, at 1564 (noting that in passing the ECPA, Congress “amend[ed] Title III to generally extend the prohibitions on interception to e-mail and crafting new protections for stored communications and stored records held by third parties.”).

70 See Mulligan, supra note 67, at 1558 (summarizing the technical and legal forces that influenced the privacy protections created by the ECPA). The first privacy concern which motivated the act was “[t]he existence of static copies of the e-mail communication’s content, which can be accessed after the fact from entities, not party to the communication[.]” Id. The second privacy concern was the “possibility that these multiple copies of e-mails, in addition to electronic files that were intentionally paced on remote commercial servers for safekeeping, were wholly without Fourth Amendment protection.” Id.

71 See id. at 1559 (explaining the consensus held by “Congress, the telecommunications and computing industry, and civil libertarians” on the inadequacy of “privacy protections for communications and stored electronic records.”).

72 See id. at 1561 (noting that Title III, which “creat[ed] a statutory right of privacy in oral and wire communications, predated the advent of electronic communications.”).

73 See id. (analyzing the goals of Title III and describing how technology has advanced to a point which makes that privacy protection inadequate). Title III was “designed to protect privacy and compensate for the uniquely intrusive aspects of electronic surveillance.” Mulligan, supra note 67, at 1561. The need for a statute focused on “aural” acquisition grew out of the fact that “[e]lectric mail and data are not ‘oral’ communications,” thus “[a]ny prohibition on intercepting electronic
Congress focused on email and data, which are of course not oral communications, and would not be covered by Title III. Additionally, the Supreme Court had not clearly determined whether Fourth Amendment protections would apply to email. In multiple cases, the Supreme Court found that individuals’ transactions were not within the scope of Fourth Amendment protections.

3. Communications Assistance for Law Enforcement Act of 1994

After eight years with the ECPA as controlling law, Congress passed the Communications Assistance for Law Enforcement Act (“CALEA”), which amended the ECPA because communications technology surpassed existing privacy protections. The crux of communications would . . . have to be based on the Fourth Amendment itself.” Id. See also Owens, supra note 39, at 187 (acknowledging that the Omnibus Crime Control and Safe Streets Act of 1968 is “generally considered Congress’s response to the Supreme Court’s holdings in Berger and Katz.”). See Mulligan, supra note 67, at 1563 (detailing the Congressional situation, which was focused on the “uncertain legal status for electronic communications and other records processed and housed on servers owned by third parties.”). Congress was motivated to enact the ECPA due to “fundamental weaknesses” highlighted “by new technical standards, laws and business models. . . .” Id. at 1559.

See id. at 1562 (recounting the lack of clarity regarding the applicability of Fourth Amendment privacy protections for electronic communications). See also Kevin McLaughlin, The Fourth Amendment And Cell Phone Location Tracking: Where Are We?, 29 HASTINGS COMM. & ENT. L. J. 421, 428 (2007) (noting that, in addition to questions on privacy surrounding electronic mail, the ECPA – and its frequent amendments to keep up with changes in modern technology, have created “ambiguous, overlapping guidance in the area of cell phone location tracking.”).

See id. at 1562 (detailing the general findings of the “business records cases,” which did not extend Fourth Amendment protections to business records, like tax, bank, and phone call records). The business records cases establish that personal information voluntarily disclosed to a business is not within the scope of the Fourth Amendment. Id. See also Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (explaining that there is no actual expectation of privacy in the phone numbers one dials, and the installation and use of a pen register was not a search); U.S. v. Miller, 425 U.S. 435, 446 (1976) (holding no Fourth Amendment privacy protections for business records given to a bank); Couch v. U.S., 409 U.S. 322, 335 (1973) (finding there is no Fourth Amendment expectation of privacy between an accountant and their client).

See Communications Assistance for Law Enforcement Act, FCC (Sept. 14, 2021), archived at https://perma.cc/QF9M-UR44 (explaining generally that “CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic
CALEA protections is the requirement that telecommunications providers make their networks technologically capable of access by law enforcement officials. The act does not extend to government wiretapping powers. CALEA grants some level of location tracking, and has presented serious Fourth Amendment concerns, considering that a person’s cell phone is generally with them inside of their home. As demonstrated in Kyllo v. United States, as far as location-based privacy is concerned, the sanctity of the home is greater than any other place.

III. Premise/Facts

Privacy concerns for big data companies and AI in the age of smartphones are some of the biggest concerns in America today. The surveillance while protecting the privacy of information outside the scope of the investigation.”). Barbara J. Van Arsdale, J.D., Construction and Application of Communications Assistance for Law Enforcement (CALEA), 47 U.S.C.A. §§ 1001 to 1010, 25 A.L.R. Fed. 2d 323, (2008) (providing that CALEA “clarifies the duty of telecommunications carriers to cooperate in intercepting communications for law enforcement purposes.”).

78 See Van Arsdale, supra note 77 (summarizing CALEA: “The telecommunications carriers must provide equipment, facilities, or services that will allow the government to intercept the wire and electronic communications of a specific subscriber without intercepting the communications of others.”).

79 See id. (explaining that “CALEA does not affect the scope of the government’s wiretapping powers. Those powers instead come from the Omnibus Crime Control and Safe Streets Act and the Foreign Intelligence Surveillance Act.”).

80 See McLaughlin, supra note 75, at 437–38 (considering the problem of cell phone tracking when the cell phone is in a private place).

This presents a major problem in the context of cell phone location tracking. Cell phones are constantly in and out of private places – most commonly homes – where no law enforcement agent could intrude without a warrant. It would be extremely difficult to track a suspect via cell phone only while he was outside the home... Id. at 438.

81 See Kyllo v. United States, 533, U.S. 27, 34 (2001) (detailing a case involving a search of the home using a technology – thermal imaging – which was found to be an invasion of privacy and a search for purposes of the Fourth Amendment). The Court held that even if “no ‘significant’ compromise of the homeowner’s privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.” Id. at 40.

82 See Lance Whitney, Data privacy is a growing concern for more customers, TECHREPUBLIC (Aug. 17, 2021) archived at https://perma.cc/KDL5-J4JA (articulating the different views on data collection, which consumers often feel “is
common practice among tech companies of collecting sensitive, user data, exacerbated further by a general consumer sense of mistrust, makes this a major concern. As more of modern life is lived through screens and other AI outfitted technology, AI concerns continue to grow. AI is new, and therefore largely unregulated and unlegislated. The American public is becoming further accustomed to granting access to personal data, while simultaneously watching the heads of social media companies testify before Congress for issues involving data collection and privacy breaches. There is a constant 

an invasion of their privacy and a practice that can be easily abused, leading to mistrust and suspicion of many businesses."). “Consumers aren’t just fearful about the practice of collecting data, they’re worried about how their data may be compromised or sold to other parties.” Id. See also Guy Pearce, Beware the Privacy Violations in Artificial Intelligence Applications, ISACA (May 28, 2021) archived at https://perma.cc/LLA9-3EMP (articulating that the challenge of protecting privacy in AI concerns how to create suitable regulations that protect privacy).

See Pearce, supra note 82 (noting that while consumer anxiety over data collection grows, use of the technology has increased); THINKML TEAM, Is Artificial Intelligence a Threat to Privacy, THINKML (Sept. 19, 2021), archived at https://perma.cc/7Q9H-GN3W (commenting that “[a] study conducted by Shields in 2018 revealed that consumers love digital assistants’ features of home security but also have apprehensions of privacy violations caused by these devices.”).

See Kathleen Walch, How and why are our devices listening to us? TECHTARGET (Jan. 31, 2020), archived at https://perma.cc/2GZL-WX38 (expanding on the idea of a continually evolving AI technology, and the need to consider the privacy and ethical implications). “Social media, government services, conversations, online meetings and group calls all spread out our personal data and increase the risk that it could be flowing into areas at risk of large-scale data breaches and privacy invasions.” Id.

See Newman, supra note 18 (listing recent cases involving AI, as well as the limited advances in AI legislation); Legislation Related to Artificial Intelligence, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 5, 2022), archived at https://perma.cc/K6SZ-KLPM (demonstrating generally the status of all bills relating to artificial intelligence back to 2019, a large portion of which failed).

See Walch, supra note 84 (expounding on the potential risks that come with AI in our devices which is programed to listen to conversations). “Users are more comfortable with voice assistants listening when explicitly consenting to the service.” Id. See also Alvin Chang, The Facebook and Cambridge Analytica scandal, explained with a simple diagram, VOX (May 2, 2018), archived at https://perma.cc/6V6E-WA48 (explaining generally the Facebook and Cambridge Analytica scandal, where Cambridge Analytica, a political consulting firm, accessed the data of up to 87 million Facebook users while working on the Trump Campaign); Paolo Zialcita, Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal, NPR (Oct. 30, 2019), archived at https://perma.cc/VLS4-WTMV (detailing
danger for abuse with AI, not only by the companies using it, but by third parties, hackers, and even the AI itself, which is why it is pertinent to ask these questions and begin taking necessary action.  

A. Artificial Intelligence

1. Applications and the Popularity of Speech Recognition Technology

The popularity of speech recognition technology is skyrocketing. Speech recognition technology is seen most notably in smart-home virtual assistant devices like the Amazon Echo. This the fines that Facebook had to pay to the U.K’s Information Commissioner’s Office following the fallout from the Cambridge Analytica scandal).


Another example is surveillance – which you could argue has potential positive benefits. But the dangers of abuse, especially by authoritarian governments, are very real. Essentially, AI is a tool that can be used by those in power to keep that power, and to increase it. Another issue is that AI can amplify discrimination and biases, such as gender or racial discrimination, because those are present in the data the technology is trained on, reflecting people’s behavior. Id. See also Walch, supra note 84 (detailing the substantial growth in the use of AI capability which fuels “society’s continued trepidations regarding privacy protections.”). “It’s expected that there will be over 7 billion AI-powered digital assistants in 2020 . . . ” Id.

88 See Ria Kuruvilla, BETWEEN YOU, ME, AND ALEXA: ON THE LEGALITY OF VIRTUAL ASSISTANT DEVICES IN TWO-PARTY CONSENT STATES, 94 WASH. L. REV. 2029, 2031 (2019) (noting the market for home devices that use speech recognition technology is growing and expected to reach $19.6 billion by 2025); Tom Dotan & Reed Albergotti, Amazon Echo and the Hot Tub Murder, THE INFO. (Dec. 27, 2016), archived at https://perma.cc/LM45-2BCC (explaining further the popularity of the Amazon Echo, which Amazon sold out of during the holiday season in 2016); Lang & Benessere, supra note 1, at 10 (noting the Microsoft’s Cortana intelligent assistant had 145 million users after three years in the market, while Apple’s Siri had an estimated 41.4 million active users in January of 2018).

89 See Kuruvilla, supra note 88, at 2032–33 (quoting the technology sector’s definition of speech recognition technology as “the ability to speak naturally and contextually with a computer system in order to execute commands or dictate language.”). “[I]t is common for a device to accidentally begin recording because it mishears the wake word.” Id. See also Impact of artificial intelligence in speech
recording technology is much less discreet than Protect Mode because virtual assistants are conspicuous to all in the room, whether by the on light when recording, or by activation at the owner’s verbal command. Requiring the user to interact with the device they willingly installed in their home means any guest in the home is likely to be aware of a virtual assistant that can “understand” human speech.

Citizen Protect Mode uses AI to record and monitor sounds around the user, looking for signs that the user is in danger and authorities should be notified. There are many companies using AI to decode audio data for virtual assistant products, with the most popular being the Amazon Echo, with Alexa technology. Alexa uses “speech recognition technology” that enables the product to execute commands based only on the user’s words.

recognition technology, INFOHOLIC RSCH. (Dec. 2019), archived at https://perma.cc/53BR-Y2HD (noting the capabilities of devices like the Amazon Echo and the Google home, which both have technology to convert voice messages to text and recognize an individual based on their voice command).

See Dotan & Albergotti, supra note 88 (detailing how an Amazon Echo, like other smart home devices, activates when it hears a “wake word” and is only recording after the wake word is detected). It is important to remember that “devices that are always listening are emerging as a new tool for police, raising the prospect of more battles between tech companies and law enforcement.” Id. See also Kuruvilla, supra note 88, at 2033–34 (demonstrating just how conspicuous the Amazon Echo is, by noting that “[w]hen an Echo is recording, the light ring on it becomes blue. The light ring turns other colors depending on its current state and function . . . . ”).

See Lang & Benessere, supra note 1, at 11 (noting the fundamental difference between installing a recording device in your home as it pertains to privacy expectations and being a guest in a home where a recording device is installed).

See Binder, supra note 13 (detailing the basic concept and functionality of Citizen’s Protect Mode); Morrison, supra note 5 (explaining how Citizen uses AI to listen for sounds of distress, then asks the user if they would like to be connected to an agent, and automatically connects the user if they don’t respond quickly enough).

See Lang & Benessere, supra note 1, at 10 (listing the most recognizable smart home devices that use technology capable of listening for – and responding to – voice commands). The massive tech companies generally “believe that voice commands and intelligent assistants will be[co]me the primary ways in which people interact with technology, possibly even more significant than touch screens and keyboards.” Id. See also Kuruvilla, supra note 88, at 2031 (noting that when comparing “companies [that] have developed virtual assistants, Amazon’s Alexa leads the pack.”). Alexa’s popularity has continually grown, with Echo-owners and daily Alexa interactions doubling in 2018. Id.

See Lang & Benessere, supra note 1, at 9 (explaining the basic functionality behind Speech Recognition Technology).
2. Present Legislation on AI That Can Record Users

Despite privacy issues, devices activated by speech and capable of executing commands remain largely unregulated federally. The lack of a comprehensive plan for the growing AI field has been recognized at least since 2016, when the Executive Office of the President for the departing Obama administration filed the report “Preparing For The Future Of Artificial Intelligence.” At the state level in 2021, bills or resolutions on general AI concerns were introduced in at least seventeen states, and became law in four.

Internationally, Europe is the gold standard for legislating data collection capabilities, with comprehensive legislation well beyond that found in the United States. The European Union’s General Data Protection Regulation (GDPR) is considered as “the toughest privacy and security law in the world.” The GDPR considers internet users to be data subjects, and grants data subjects eight rights, which include the right to be informed, the right to erasure, and the right to object. See also Eve Gaumond, Artificial Intelligence Act: What Is The European Approach for AI?, LAWFARE (June 4, 2021), archived at https://perma.cc/QA99-C4JF (understanding that the EU is taking charge of this legislation, and advocating that “[t]he international community should not let Europe write the rules that govern technology all by itself.”). “[T]he United States should play an active role in helping Europe to develop a balanced and nuanced regulatory framework for AI.” Id. The EU has invited the United States to “start acting together on AI . . . .” Id.

---

95 See Kuruvilla, supra note 88, at 2040 (considering the limited present state of regulation at the federal level for devices that listen to their human users). See also Yoon Chae, U.S. AI Regulation Guide: Legislative Overview and Practical Considerations, 3 J. ROBOTICS, A.I. & L. 17, 17 (2020) (explaining that “[r]egulation of artificial intelligence (“AI”) is still in its infancy.”). “Much of the recent development in filling the legal void that exists for AI governance is surprisingly coming from the United States, which, with the exception of three AI reports issued by the Obama administration, has been relatively inactive with AI regulation . . . .” Id.


97 See Legislation Related to Artificial Intelligence, supra note 85 (summarizing the most recent tally of bills and resolutions introduced from 2019–2021). The legislative action taken in 2021 across various states is not necessarily related to devices that record human interactions, but rather focuses generally on “[c]oncerns about potential misuse or unintended consequences of AI . . . .” Id. The list of states which enacted general artificial intelligence bills or resolutions in 2021 is Alabama, Colorado, Illinois, and Mississippi. Id.

98 See Ben Wolford, What is GDPR, the EU’s new data protection law?, GDPR.EU (Nov. 21, 2021), archived at https://perma.cc/E4D5-AC34 (providing a general overview of the General Data Protection Regulation (“GDPR”), which is described as “the toughest privacy and security law in the world.”). The GDPR considers internet users to be data subjects, and grants data subjects eight rights, which include the right to be informed, the right to erasure, and the right to object. Id. See also Eve Gaumond, Artificial Intelligence Act: What Is The European Approach for AI?, LAWFARE (June 4, 2021), archived at https://perma.cc/QA99-C4JF (understanding that the EU is taking charge of this legislation, and advocating that “[t]he international community should not let Europe write the rules that govern technology all by itself.”). “[T]he United States should play an active role in helping Europe to develop a balanced and nuanced regulatory framework for AI.” Id. The EU has invited the United States to “start acting together on AI . . . .” Id.
Protection Regulations (“GDPR”) was passed in 2018, and reaches far beyond Europe, to any organization that collects data related to EU citizens. Legislators in the EU have also been working on the “Artificial Intelligence Act,” a GDPR style regulatory system which “addresses the risks stemming from the various uses of AI systems and aims to promote innovation in the field of AI.”

“The Automatic Listening and Exploitation Act,” also known as the ALEXA Act, was introduced to target recording devices in the home. The act, from Massachusetts Rep. Seth Moulton, was inspired partly by the Facebook Cambridge Analytica scandal, where personal data of millions of Facebook users was collected, without consent, for political advertising. This act grew from a desire to keep pace with European lawmakers’ efforts to legislate digital privacy laws. The bill was introduced in 2019 and referred to the Subcommittee on Consumer Protection and Commerce but was not

---

99 See Wolford, supra note 98 (expressing that the privacy laws within the GDPR apply to any organization that does any amount of data collection). “The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.” Id. See also THINKML TEAM, supra note 83 (commenting that “Europe’s GDPR in 2018 ushered new standards on an individual’s right to his private information and hence domed digital privacy expectation to the next level.”).

100 See Gaumond, supra, note 98 (explaining the EU plan to approaching legislation for AI). The EU has taken a staggered approach for their AI regulations, choosing to classify different AI technology with different levels of regulation, with unacceptable risk being banned entirely and no risk being left alone. Id. Makena Kelly, Seth Moulton tackles Alexa data collection with new bill, The VERGE (July 24, 2019) archived at https://perma.cc/PQR2-P3TJ (quoting Rep. Moulton that Congress should give Americans a bigger say in the data that companies collect.”). “‘It’s time for a next generation of digital privacy laws, and it can start by holding corporations to their own privacy commitments.’” Id.

101 See Kelly, supra note 100 (detailing the general concept behind the ALEXA Act, which is to “empower the Federal Trade Commission to seek immediate penalties if a smart device is found to have recorded user conversations without the device’s wake word being triggered.”). The proposed bill would allow the FTC to seek as much as $40,000 in penalties from each offending company, per infraction. Id.

102 See id. (explaining Rep. Seth Moulton’s intention to pass a bill “that would limit how smart device manufacturers like Amazon and Google can collect your data.”). “In the aftermath of Facebook’s Cambridge Analytica scandal, both chambers of Congress have reportedly begun to draft legislation that would create a federal data privacy framework.” Id.

103 See id. (quoting representative Moulton, who stated “The Europeans are way ahead of us, and yet we have a Senate that doesn’t even understand Facebook.”).
advanced beyond that. Rep. Moulton was also involved in the “Informing Consumers about Smart Devices Act,” which aimed to address devices with non-obvious recording capabilities which would require reasonable disclosure guidelines. This bill has also stalled, demonstrating the continued lack of legislation on digital privacy.

In addition to the ALEXA Act and the Informing Consumers about Smart Devices Act, there is another data privacy and AI initiative yet to be definitively decided: the “Algorithmic Justice and Online Platform Transparency Act of 2021,” introduced by Senator Edward Markey and Congresswoman Doris Matsui. This act would require certain threshold companies, based on revenue, to “conduct algorithmic impact assessments of their technology.” Like the acts mentioned that came before it, this one has also stalled, but the sponsors plan to reintroduce it.

---

104 See Automatic Listening Exploitation Act of 2019, H.R.4048, 116th Congress (2019) (noting that after the bill was introduced to the house, the latest (and only) action on the bill was when it was referred to the Subcommittee on Consumer Protection and Commerce).

105 See Curtis, Moulton Introduce Bipartisan Bill To Protect Consumers From Curious Smart Devices, SETH MOULTON (July 13, 2020), archived at https://perma.cc/P3HR-YY89 (explaining in a press release the introduction of the Informing Consumers about Smart Devices Act, which “requires the creation of reasonable disclosure guidelines for products that have audio or visual recording components that are not clearly obvious to a reasonable person, such as a kitchen or another household appliance.”).

The legislation is in response to reports about household devices listening to individual’s conversations without their knowledge. While some manufacturers have taken steps to more clearly label their products with listening devices, this legislation would make this information more obvious to consumers without overly burdensome requirements on producers of these devices.

106 See Informing Consumers about Smart Devices, H.R. 7583, 116th Congress (2020) (noting the status of the bill, which was introduced in the house on July 13, 2020).


108 See id. (explaining that certain companies would be required to conduct compliance activities if they have more than $50 million in revenues).

109 See id. (noting that the bill was never read in committee or on the Senate floor, but that there are plans to reintroduce the bill in both the Senate and the House this year).
A piece of legislation that passed with legitimate data privacy measures is the California Consumer Privacy Act of 2018 (“CCPA”), the furthest reaching privacy measure in the United States yet. The CCPA was passed to keep step with the GDPR, as the California legislature recognized the United States’ lack of an expansive data protection law and the need to provide a way for individuals to regain control of their personal data. The CCPA has been described as “one of the toughest data privacy laws in the country.” The CCPA was enacted because there is no federal equivalent to the EU’s GDPR. The CCPA applies to businesses that collect and sell or

110 See Joanna Kessler, DATA PROTECTION IN THE WAKE OF THE GDPR: CALIFORNIA’S SOLUTION FOR PROTECTING “THE WORLD’S MOST VALUABLE RESOURCE”, 93 S. CAL. L. REV. 99, 101–02 (2019) (explaining the strength and reach of the California Consumer Privacy Act of 2018 (“CCPA”)). The CCPA will require companies to overhaul their management of consumer’s personal data). Id. at 120. The CCPA is the toughest data privacy law in the United States, and it is likely that a future federal standard would be a “watered down version . . . .” Id. at 110. The United States does not yet have a federal equivalent to the GDPR, and any present federal data protection laws have targeted specific industries. Id. at 105. See also Is Artificial Intelligence a Threat to Privacy, supra note 83 (describing the CCPA as the “most inclusive bill to avoid privacy violation.”). “[CCPA] has set some standards to regulate privacy concerns and emphasized companies to take permission from the user before sharing their private data with others. Id. “[T]he parent company can easily observe what their users are talking about, what are they doing or about to do without even their knowledge.” Id.

111 See Kessler, supra note 110, at 101–02 (noting the differences between the expansive GDPR with the previous American legislation on data privacy). “Academics have argued that the United States ‘has a weak tradition of data privacy that is diametrically opposed to the EU’s expansive data protection laws.’” Id. (quoting Michael L. Rustad & Thomas Koenig, Towards a Global Data Privacy Standard, 71 FLA. L. REV. 365, 370 (2019)). “The California law applies even more broadly than the GDPR as it covers not only individual data, but information pertaining to households and devices as well.” Id. at 111. While the CCPA and GDPR cover overlapping areas, they differ in that the CCPA is more lenient than the GDPR, and the CCPA only applies to companies which meet minimum thresholds. Id. at 112–13.

112 See id. at 106 (articulating where the CCPA stands in comparison to the other data privacy laws in the United States). “California has been a consistent leader in the United States on the data privacy front, as it enacted the first laws requiring consumers to be notified of data security breaches and website privacy policies.” Id.

113 See Kessler, supra note 110, at 105 (mentioning that there not yet a federal equivalent to the EU’s GDPR); Bambauer, supra note 49, at 275 (commenting that “the United States stands alone among developed countries without omnibus data protection laws.”).
disclose personal information of California consumers for a “business purpose.”

3. Recording Devices in the Home

The popularity of smart home devices has predictably resulted in the recording of events which users would prefer had remained private, like a potential struggle that resulted in death. This occurred when a man was found dead in the hot tub at a home where he had been drinking as a guest the night before, potentially while the defendant homeowner’s Amazon Echo was recording. The prosecution issued a warrant demanding the recordings from Amazon when they suspected foul play had occurred. Amazon declined the request but did hand over the recordings when the defendant requested them to clear his name. While this case did not escalate to a point

---

114 See Kessler, supra note 110, at 107 (noting that “the CCPA applies to businesses that collect and sell California consumers’ personal information or disclose that information for a ‘business purpose.’”). “Under the CCPA, ‘personal information’ is any ‘information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.’”). Id. at 108.
115 See Lang & Benessere, supra note 1, at 10 (making connections to the Bates case in the state of Arkansas, where a man was found dead in the homeowner’s hot tub, and the prosecution sought recordings of the evening from Amazon, which they suspected they had, based on the presence of an Amazon Echo in the home). “We also know that Alexa can record events, such as a crime or an accident, because the Echo is equipped with seven microphones that use beam-forming technology and enhanced noise cancellation.” Id. Amazon refused the prosecution’s request, but the homeowner voluntary submitted any recordings. Id.
116 See Lang & Benessere, supra note 1, at 10 (explaining further the circumstances that led to prosecutors in the Bates case seeking Amazon Echo recordings which could have potentially included sounds from an altercation). See also Nicole Chavez, Arkansas judge drops murder charge in Amazon Echo case, CNN (Dec. 2, 2017), archived at https://perma.cc/AMM5-7HLH (recounting the facts of the Bates case, where another guest recalled hearing music at the party, which would suggest the Amazon Echo was recording and could have recorded a struggle).
117 See Chavez, supra note 116 (explaining the prosecution’s strategy in the Bates alleged murder case involving the Amazon Echo potentially recording a struggle, and the justification for their request).
118 See Lang & Benessere, supra note 1, at 10 (explaining that the privacy concern issue, and whether Amazon could be forced to turn over the recordings, went unresolved because the defendant voluntarily turned over the recordings). See also Agatha French, Q&A:: Alexa may be listening, but will she tell on you?, L.A.TIMES (Jan. 5, 2017), archived at https://perma.cc/BK9B-APAA (noting that Amazon
that determined the government’s ability or inability to obtain recordings held by an uncooperative company, this instance is emblematic of the privacy questions raised by installing recording devices in one’s own home. These devices present privacy concerns for homeowners, but the situation changes drastically when the devices record an ignorant guest.

B. Citizen Protect Mode and Privacy Concerns in the Home of a Guest and in Public

Enabling Citizen Protect Mode while a guest in another’s home is the most pressing privacy concern presented by Protect Mode, because it listens and records with the sole consent of the Citizen subscriber. The difference between smart home devices and Protect Mode is the likelihood of a complete lack of consent by the homeowner if their guest has enabled this feature on their personal phone. Fourth Amendment case law demonstrates the home is given stated they “will not release customer information without a valid and binding legal demand properly served . . . ”).

119 See Lang & Benessere, supra note 1, at 10 (noting that the case did not ultimately answer whether Amazon, the company that made the recording, was required to submit the recording to the prosecution without consent of the smart homeowner, because the owner chose to submit it on his own voluntarily).

120 See id. at 11 (noting the differences between being recorded in one’s own home on a smart home device, which the homeowner is at least aware of, and being recorded as a guest in a home equipped with a smart home device, which the guest may not be aware of, let alone consent to). Cf. Raphael Davidian, Alexa and Third Parties’ Reasonable Expectation of Privacy, 54 AM. CRIM. L. REV. ONLINE 58, 63 (2017) (speaking to the inverse of privacy concerns for homeowners, which is the privacy concern where visitor consent is lacking). “One-party consent laws will no longer be feasible in this context without an exception, as they would completely eradicate any expectation of privacy when visiting another’s home.” Id.

121 See Heater, supra note 4 (detailing the general functionality of Citizen Protect Mode, which, when enabled, monitors the user through the smartphone microphone). “When enabled . . . the app will live monitor the user’s audio feed, using AI to detect for things like screams, offering up a connection to the agent.” Id.

122 See Lang & Benessere, supra note 1, at 11 (explaining the lack of consent for a guest in a home where they don’t know there is a smart home recording). The situation with smart homes recording guests is complicated because when entering the home of another, “[e]xpectations of privacy . . . change.” Id. See also Binder, supra note 13 (examining the obvious privacy concern that accompanies Protect Mode, specifically that a third-party cannot consent to being recorded unless they are specifically alerted that the program is running). “[W]hile a Citizen Protect mode
the highest level of privacy, and if Protect Mode were triggered in the home, it is unclear if police would be sufficiently justified to search without a warrant, and whether the prosecution would have access to any recordings in an instance where charges were filed. The privacy concerns for Protect Mode are diminished in a public setting, where there is no objective expectation of privacy. This seems to be the general space Citizen intended to monitor, as evidenced by their original commercials, when still named Vigilante, which depicted situations where innocent civilians needed protection from dangerous individuals while in public.

C. Audio Surveillance Laws – State by State Variation

There are variations by state for the required consent to record a conversation, with state legislators determining that either all parties must consent, or only one must consent. In one-party consent states, individuals are allowed to record without obtaining consent from any other parties. In all-party consent states, recordings cannot be made without all parties’ consent. The customer may consent to Distress Detection, a nearby non-customer third-party could surely have concerns about the service spying or snooping on them.”

123 See Lang & Benessere, supra note 1, at 12 (noting that “[w]e are now at the start of an era in which previously unavailable data can be accessed, become discoverable and later introduced into evidence.”).

124 See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing the two-prong requirement for privacy rights). A person does not have a reasonable expectation of privacy when in public. Id. See also McClurg, Bringing Privacy Law Out of the Closet, supra note 41, at 990 (proposing tort liability for privacy intrusions, because tort law “clings stubbornly to the principle that privacy cannot be invaded in or from a public place.”).

125 See Crosbie, supra note 11 (explaining that Citizen notifies users of in-progress criminal activity in their immediate area). When still called Vigilante, a video was published showing a woman using the app for protection on an ominous city street, which was a “highly dramatized scenario showing the app at work.” Id.


127 See id. (defining one-party consent statutes). See also R.I. GEN. LAWS § 11-35-21 § (c)(3) (2012) (demonstrating an example of a one-party consent statute). In Rhode Island, “a person not acting under color of law to intercept a wire, electronic, or oral communication, where the person is a party to the communication, or one of the parties to the communication has given prior consent to the interception unless the communication is intercepted for the purpose of committing any criminal or tortious act . . . .” Id.
without consent from every member of the conversation.\textsuperscript{128} Presently, thirty-eight states follow one-party consent statutes, and twelve follow all-party consent statutes.\textsuperscript{129}

Citizen is nationwide, but only offers real-time crime alerts in roughly sixty cities.\textsuperscript{130} Citizen’s website offers twenty-nine examples, spanning nineteen states, as well as Washington D.C.\textsuperscript{131} Of those, six are all-party consent states and fourteen are one-party consent states.\textsuperscript{132} Citizen’s service can potentially violate wiretapping statutes and must be conscious of where their product is used to avoid violating recording statutes in an all-party consent statute state.\textsuperscript{133}

IV. Analysis

Personal privacy has long been a concern in America.\textsuperscript{134} While the Fourth Amendment applies to protections from unreasonable searches and seizures from the government, it is this foundational

\textsuperscript{128} See Audio Surveillance Laws by State, \textit{supra} note 126 (defining all-party consent statutes). \textit{See also} MASS. GEN. LAWS ch. 272, § 99(4) (2022) (establishing that Massachusetts is an all-party consent state, meaning every person must be aware if they are being recorded). The Massachusetts Wiretapping Statute makes it illegal to “secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication. . . .” Id.

\textsuperscript{129} See Audio Surveillance Laws by State, \textit{supra} note 126 (categorizing the states based on whether they follow one-party consent statutes or all-party consent statutes for recording conversations).

\textsuperscript{130} See \textit{Where is Citizen available?}, CITIZEN (Feb. 19, 2023), archived at https://perma.cc/3AYZ-L9GY (explaining that the Citizen application is available nationwide, but it is only in specific cities where the content of the app is curated by Citizen employees).

\textsuperscript{131} See \textit{id.} (showing that Citizen Protect Mode is available in sixty cities in the United States and listing twenty-nine of those cities).

\textsuperscript{132} See \textit{id.} (listing twenty-nine cities where Citizen is available). \textit{See also} Audio Surveillance Laws by State, \textit{supra} note 126 (listing all states by their statutes as one-party consent states or all-party consent states).

\textsuperscript{133} See \textit{id.} (defining all-party consent statutes, which hold that “recording cannot be done without the consent of every member of the conversation).

\textsuperscript{134} See generally Warren & Brandeis, \textit{supra} note 36, at 193 (noting their 1890 Harvard Law Review article “The Right to Privacy,” which is a foundational writing on the topic, over a century later); Prosser, \textit{supra} note 41, at 383 (recounting the California Law Review article which progressed the right to privacy further). \textit{See also} U.S. CONST. amend. IV (articulating a constitutional right to be free from unreasonable searches and seizures from governmental bodies).
privacy expectation that requires fresh conversations on advancing AI technology utilized by private companies, so consumers may have legal recourse when their privacy is invaded.\textsuperscript{135} Citizen’s pushing of privacy boundaries raises questions of legality when used in the home of someone who is unaware the application is running, and furthermore creates potential for malicious purposes.\textsuperscript{136} The potential answers suggest that Citizen’s team needs to address their app’s potential for intrusion upon seclusion.\textsuperscript{137} Additionally, if Citizen does not alter their product, and other similar speech recognition products increase in prevalence, then the invasion of privacy torts must be expanded to address this issue.\textsuperscript{138} Protect Mode creates a problem that is most troubling in all-party consent states because a subscriber in the home of another most likely will not alert the homeowner of the surveillance because that would disrupt the purpose of the app.\textsuperscript{139} Protect Mode listens for signs of distress and then alerts a Protect agent, but the potential for mishaps is substantial, as the AI could mistakenly detect distress from a scream in a horror film, a gunshot in an action movie, or even consensual acts in the bedroom.\textsuperscript{140}

\textsuperscript{135} See U.S. CONST. amend. IV (quoting the text of the Fourth Amendment, which is the basis for the individual’s right to privacy from government actors). See also THINKML TEAM, supra note 83 (noting the new tendency for businesses to become more intrusive with their technology as that technology advances).

\textsuperscript{136} See Morrison, supra note 5 (explaining the features of the Citizen app, but also the potential issues with such a surveillance technology used for illicit purposes); Owens, supra note 39, at 178 (articulating the question as to how illegal eavesdropping evidence, obtained by a citizen and given to authorities, is to be dealt with during a follow-up investigation).

\textsuperscript{137} See generally THINKML TEAM, supra note 83 (speaking on the necessity for companies to limit themselves and adopt technical approaches when dealing with issues on data privacy).

\textsuperscript{138} See Richards & Solove, supra note 41, at 1924 (noting that the privacy torts which Prosser codified have been locked into their current form since their addition to the Second Restatement of Torts, rendering them “woefully inadequate to address the privacy problems we face today.”). “It is time for the tort law of privacy to regain the creative spirit it once possessed. It must do so if it is to remain relevant to protect privacy in today’s Information Age.” Id. “[T]o be vital in the future, the law of tort privacy must move beyond Prosser’s conception of privacy.” Id. at 1891.

\textsuperscript{139} See Audio Surveillance Laws by State, supra note 126 (explaining that a state that follows an all-party consent statute means that “recording cannot be done without the consent of every member of the conversation.”). See also Owens, supra note 39, at 177–78 (asserting the difference between eavesdropping and wiretapping by someone other than the government, like a business associate or a curious neighbor).

\textsuperscript{140} See Binder, supra note 13 (noting that Citizen’s Distress Detection “is a mode which allows Citizen’s AI-technology to monitor audio through your phone.”). “If
A. Citizen’s Protect Mode Third Party Invasion of Privacy Implications

Citizen Protect Mode, when engaged in another’s home, should be considered an intrusion upon seclusion for the homeowner if they are not informed that they are being recorded. Until Citizen fully partners with the police, which has been considered and decided against by some police departments, this problem falls outside of Fourth Amendment considerations, because Citizen is not a government actor. Instead, Protect Mode creates invasions of privacy under tort law, specifically Prosser’s first privacy tort, intrusion upon the plaintiff’s seclusion or solitude. Protect Mode intrudes as it monitors for audio cues of distress, and if triggered, then a third-party agent can listen into the homeowner’s private affairs. While this is a tort violation under Prosser’s tort of intrusion, it is also

it detects a ‘distress signal,’ such as a scream, the app will ask if you want to be connected to an agent.”

141 See Richards & Solove, supra note 41, at 1898 (detailing Prosser’s understanding of the right to privacy).

Most courts now recognize the existence of a right of privacy, which will be protected against interferences which are serious and outrageous, or beyond the limits of common ideas of dangerous conduct. The right has been held to cover intrusions upon the plaintiff’s solitude; publicity given to his name or likeness, or to private information about him; placing him in a false light in the public eye; and the commercial appropriation of elements of his personality. The right is subject to a privilege to publish matters of news value, or of public interest of a legitimate kind.

142 See Cox & Koebler, supra note 16 (recapping the events which led to the LAPD choosing not to establish a relationship with Citizen after Citizen set off a manhunt by offering a bounty for an innocent man). See also U.S. CONST. amend. IV (articulating a constitutional right to be free from unreasonable searches and seizures from governmental bodies).

143 See Prosser, supra note 41, at 389 (articulating the first of his synthesized privacy torts, Prosser explained “[i]ntrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.”). This intrusion tort is meant to address a mental interest. Id. at 392.

144 See Binder, supra note 13 (noting that through Citizen’s Distress Detection “a nearby non-customer third-party could surely have concerns about the service spying or snooping on them.”).
a violation of wiretap statutes in all-party consent states, presuming the homeowner has not been alerted of the Protect Mode feature.\textsuperscript{145} It is debatable if this is a violation of wiretap statutes in one-party consent states, because even though the recording in this hypothetical is taking place in the home of another, only one-party is required to consent to recording.\textsuperscript{146} Since there has yet to be an incident where Protect Mode created an exigent circumstance for police to enter a home without the requirement of a warrant, it is concerning because it seems so plausible, as exigent circumstances can be justified by an officer’s reasonable belief.\textsuperscript{147} There has also not yet been an incident where an invasion of privacy tort has been asserted against Citizen for recording without consent, but the potential is there and is why the tort of intrusion must be modified.\textsuperscript{148}

\textsuperscript{145} See Prosser, supra note 41, at 390 (articulating the first of his synthesized privacy torts, Intrusion, which “carried beyond such physical intrusions . . . [and] was extended to eavesdropping upon private conversations by means of wire tapping and microphones . . . ”). “It is clear also that the thing into which there is prying or intrusion must be, and be entitled to be, private.” Id. at 391. “[T]he interest protected by this branch of the tort is primarily a mental one. It has been useful chiefly to fill in the gaps left by trespass, nuisance, the intentional infliction of mental distress, and whatever remedies there may be for the invasion of constitutional rights.” Id. at 392. See also Owens, supra note 39, at 190 (noting individual’s privacy rights under Title III).

\textsuperscript{146} See Audio Surveillance Laws by State, supra note 126 (explaining the difference between one-party consent state and all-party consent states). States that follow “one-party consent” statutes “allow individuals to record conversations with their knowledge, but do not require them to tell the other party.” Id.

\textsuperscript{147} See Binder, supra note 13 (detailing how the Citizen Protect Mode functions, which involves AI technology listening to the sounds surrounding the user through the phone microphone and monitoring for sounds of distress). See also Huff, supra note 28, at 379--80 (explaining that while the Fourth Amendment jurisprudence has drawn a line at the door to the home for warrantless searches, exigent circumstances create an exception where “‘real immediate and serious consequences’ will ‘certainly occur’ if a police officer postpones action to obtain a warrant.’”).

\textsuperscript{148} See Richards & Solove, supra note 41, at 1924 (arguing the necessity of strengthening the invasion of privacy torts, because “[i]f the tort law of privacy is to survive in the twenty-first century, it must finally emerge from Prosser’s shadow and regain some of Warren and Brandeis’s dynamism.”). For tort law to adjust to modern
B. Potential Alterations to the Citizen App to Avoid Invasions of Privacy

The Citizen app functions by using location services of the user to alert them of danger in their area.\textsuperscript{149} Since Protect Mode is monitoring the exact location of the user in real time when they have the feature engaged, Citizen should also be able to know when the customer has entered a private residence, and theoretically put in some sort of pause feature.\textsuperscript{150} Of course, this disrupts Citizen’s entire business model.\textsuperscript{151} People want to pay $19.99 per month to be protected at all times, not just in public.\textsuperscript{152} Therefore, it seems unlikely that Citizen will modify their app to stop doing exactly what it is advertised and designed to do as soon as the user enters a home that is not their own.\textsuperscript{153}

privacy concerns, it “must rethink antiquated understandings of privacy . . . [and] abandon the binary, all-or-nothing approach toward privacy in favor of a more modern and nuanced understanding of the gradations between purely public and purely private.” \textit{Id.} at 1922. \textit{See also} McLaughlin, \textit{supra} note 75, at 438 (commenting that “[h]owever, unforeseen advancements in technology may make such particular, outside-only tracking feasible,” which suggests that the technology does exist for Citizen to turn off and on the surveillance mechanism inside the home).\textsuperscript{149} \textit{See} Morrison, \textit{supra} note 5 (explaining the Citizen sends out “push alerts to users when things like fires, car accidents, and crimes happen in their area.”). \textsuperscript{150} \textit{See id.} (explaining that Citizen “can be used as a sort of digital bodyguard to monitor you if you’re in a potentially unsafe situation.”). “[Citizen is] able to detect your precise location in real time.” \textit{Id.} \textit{See also} McLaughlin, \textit{supra} note 75, at 438 (articulating a similar concern surrounding cell phone surveillance in and out of the home while complying with the Fourth Amendment). “It would be extremely difficult to track a suspect via cell phone only while he was outside the home, but never while he was inside the home[.]” \textit{Id.}\textsuperscript{151} \textit{See Morrison, supra} note 5 (stating that the Citizen subscription service “gives subscribers access to an on-demand Protect Agent, who they can call upon if they think they need – or might need – emergency assistance.”). \textsuperscript{152} \textit{See id.} (explaining that the users of the Citizen Protect Mode are paying specifically for this service that monitors them at all times when they have the feature engaged).\textsuperscript{153} \textit{See Flood, supra} note 13 (recounting a statement made by CEO Andrew Frame where he stated that Citizen is not meant only for emergencies, but to give people “peace of mind” in their daily lives). Citizen’s Medium blog mentions example scenarios that the application was designed for, such as “[a] solo walk home at night and a disastrous first date.” \textit{Id.} \textit{See also} McLaughlin, \textit{supra} note 75, at 438 (noting that outside-only tracking is feasible thanks to technological advancements, which suggests Citizen could be tweaked to monitor only outside of the home).
The issue of Protect Mode in homes where the user is a guest appears in all-party consent states.\textsuperscript{154} While there are fewer all-party consent states than one-party consent states, removing the Protect Mode feature from the app in those states would be a major market hit to Citizen.\textsuperscript{155} Of the nineteen states, and Washington D.C., where Protect Mode is available, six have all-party consent statutes.\textsuperscript{156} If Citizen is unable or unwilling to alter their application to mitigate the problem regarding unauthorized surveillance in homes in all-party consent states, the risk of the tort of intrusion is substantial enough that the app should be discontinued.\textsuperscript{157}

C. Proposal for Expanding and Strengthening the Invasion of Privacy Torts

The tort of intrusion, needs updating and strengthening to keep up with advances in technology and address the privacy concerns

\textbf{[T]he only option for evading tracking is to turn off the cell phone, or at a minimum to not make or receive any calls. But turning off the phone strips the phone of the ability to receive inbound calls, and protecting oneself by not using the phone simply fails to recognize the reality of cell phone usage in modern life.}}

\textit{Id. at 441.}

\textsuperscript{154} See \textit{Audio Surveillance Laws by State}, supra note 126 (explaining that all-party consent states require that all members of the party need to be aware that the conversation or activity is being recorded).

\textsuperscript{155} See \textit{id.} (listing off the states that are all-party consent states). \textit{See also Where is Citizen available?}, supra note 130 (listing the 19 states (and Washington D.C.) where Citizen Protect Mode is available).

\textsuperscript{156} See \textit{Audio Surveillance Laws by State}, supra note 126 (listing states by whether they are all-party consent states or one-party consent states); \textit{Where is Citizen available?}, supra note 130 (showing a list of states where Citizen Protect Mode is available).

\textsuperscript{157} See Prosser, supra note 41, at 390 (expanding on the requirements for the intrusion of privacy tort, which “carry[es] beyond such physical intrusion[,]” extending to “eavesdropping upon private conversations by means of wire tapping and microphones[,]”).

\textit{It is clear also that the thing into which there is prying or intrusion must be, and be entitled to be, private . . . On the public street, or in any other public place, the plaintiff has no right to be alone, and it is no invasion of his privacy to do no more than follow him about.}}

\textit{Id. at 391.}
presented by Citizen Protect Mode. Independent of whether Citizen modifies their app to avoid invasion of privacy issues, the concern for the legality of Citizen Protect Mode in homes of non-consenting parties suggests that those homeowners need an avenue of recourse against either the person using the Citizen service, Citizen, or both. This is where modifications or a complete overhaul to the invasion of privacy torts comes into play. Tort law could be the driver of company policy because it can be written as a deterrent for companies that utilize this technology, ensuring they create products which protect the consumer and avoid invasion of privacy tort actions in the first place.

The tort of intrusion upon seclusion, to make it a more suitable recourse for invasions of privacy perpetrated through an app like Citizen, should be rewritten to remove the high bar for “highly offensive to a reasonable person.” This could certainly be

---

158 See Richards & Solove, supra note 41, at 1924 (noting that the privacy torts which Prosser codified have been locked into their current form since their addition to the Second Restatement of Torts, rendering them “woefully inadequate to address the privacy problems we face today.”); Prosser, supra note 41, at 389 (detailing the intrusion portion of the law of privacy as “[i]ntrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.”). See also Owens, supra note 39, at 191 (articulating what is a convincing reason to strengthen the intrusion upon seclusion tort, specifically that “[t]here are no Fourth Amendment protections against eavesdropping by one’s curious neighbor.”).

159 See Bambauer, supra note 49, at 209 (suggesting that “[t]he intrusion tort is the quintessential example of a restriction on observation.”). The Intrusion upon Seclusion, with minor adjustments, is a potential avenue of recourse, because, “[i]ntrusion has great, untapped potential to address privacy harms created by advances in information technology. Though the tort is associated with conduct in real space, its principles apply just as well to operations in the era of Big Data.” Id. at 207. “[T]he intrusion tort imposes liability for obnoxious observations, as opposed to the creation of data, [thus] . . . the intrusion tort is apt to deter offensive, targeted observations, and to protect the sense of seclusion that people have come to expect even in a world brimming with data.” Id. at 275.

160 See id. at 273 (concluding that “[t]ort law holds the solution to vexing problems in privacy law. Yet it has been neglected by privacy law scholars, who are on a misguided quest to constrain the quantity, spread, and repurposing of personal data.”).

161 See id. at 275 (determining “that the intrusion tort imposes liability for obnoxious observations, as opposed to the creation of data . . . demonstrating that the intrusion tort is apt to deter offensive, targeted observations, and to protect the sense of seclusion that people have come to expect even in a world brimming with data.”).

162 See RESTATEMENT (SECOND) OF TORTS: INTRUSION UPON SECLUSION § 652B (1977) (highlighting the present burden a plaintiff must satisfy to establish defendant
considered a drastic measure which could lead to considerable litigation for minor issues, but this proposal is meant more to put developers of these products on notice that any invasion of privacy (like this Citizen hypothetical) will lead to litigation and damages. This proposed alteration is meant to be severe and act as a placeholder until the U.S. adopts a federal standard similar to the GDPR.

D. Unification of Electronic Surveillance and Data Protection Regulation in the U.S.

The electronic surveillance Citizen provides through Protect Mode highlights the lack of a cohesive data protection regulation in the United States. Citizen, a private company, seems unconstrained liability for an invasion of privacy); Meltz, supra note 56, at 3439 (recounting the Restatement (Second) of Tort’s Formulation of Intrusion Upon Seclusion). “It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.” Id. See also Zhu, supra note 23, at 2411 (noting that the tort of intrusion requires the plaintiff to overcome the offensiveness requirement, and as presently written and enforced, “the offensiveness of any privacy intrusion turns on . . . contextual judgments.”).

See Bambauer, supra note 49, at 256 (justifying damages for tort law invasions of privacy, by stating that “[a] primary goal of tort law— and especially the law of intentional torts—is to deter socially repugnant behavior.”). “Intrusion liability rules will create much-needed clarity of law and policy . . . so long as [businesses] stay within the bounds of per se objectively reasonable observation.” Id. The modification to “[i]nterception law would put an end to many problematic practices without forcing online businesses to significantly alter their websites, and without undermining the revenue model that currently supports much of the free online content.” Id. at 257.

See id. at 275 (noting that “the United States stands alone among developed countries without omnibus data protection laws[.]”). See also Kessler, supra note 110, at 105 (stating the “[i]n the United States, there is not yet any federal equivalent to the GDPR.”).

See Kessler, supra note 110, at 101–02 (explaining the historical lack of a cohesive data protection regulation in the United States, in addition to the fact that “the United States does not recognize a fundamental right to privacy.”). “[I]t is clear that the emphasis on data privacy is being embraced around the globe. Jurisdictions around the world are enacting legislation to conform to the EU’s GDPR, due both to the law’s extraterritorial application and the other countries’ recognition of the importance of data privacy.” Id. at 121.

Since it has been anticipated that other states would follow California’s lead and pass laws similar to the CCPA, large technology companies are concerned about having to comply with a patchwork system of laws, which will likely be more expensive
by the Fourth Amendment, and the insufficiency of present tort recourse is a problem that remains to be fully addressed.\textsuperscript{166} This highlights the necessity for an expansion of data privacy regulations, in the vein of those spearheaded by California with their passing of the CCPA.\textsuperscript{167} The CCPA applies to the sort of data that Citizen collects, which includes geolocation data and audio information.\textsuperscript{168} Enacting federal legislation to match California’s, which was enacted to match the GDPR in Europe, will render the previously mentioned expansion of the invasion of privacy torts more of a supplemental measure, to be used only when companies run astray of the data privacy regulations.\textsuperscript{169}

\section*{V. Conclusion}

Citizen has inadvertently created a product that is prime for misuse and invasions of privacy. While the search and seizure potential may initially seem to suggest this is a Fourth Amendment issue, this is more of an issue for privacy legislation and regulations. Enacting a strong, unified legislation to protect the data privacy of American consumers, like the GDPR in the EU and the CCPA in California, would make the greatest difference, because there would

\begin{quote}
and burdensome than compliance with one state’s standard. As a result, several technology companies have said they would embrace a federal privacy law . . . .
\end{quote}

\textit{Id.} at 122–23.\textsuperscript{166} See Richards & Solove, \textit{supra} note 41, at 1924 (concluding that present tort law is insufficient for the problem of addressing invasions of privacy issues arising from data privacy intrusions). To alter invasion of privacy torts for the twenty-first century relevance, it is necessary to move away from the Prosser invasion of privacy torts, and “regain some of Warren and Brandeis’s dynamism.” \textit{Id.} “It is time for the tort law of privacy to regain the creative spirit it once possessed. It must do so if it is to remain relevant to protect privacy in today’s Information Age.” \textit{Id.}\textsuperscript{167} See Kessler, \textit{supra} note 110, at 122 (noting that California has led the way in this area of data privacy legislation).\textsuperscript{168} See \textit{id.} at 108 (explaining that the CCPA applies not only a wide range of businesses, but also to a wide range of types of collected information). “[T]he requirements imposed by the CCPA are substantial, and therefore businesses will need to make significant changes to ensure they are complying with the law. Companies will also need to update their privacy policies to incorporate the new rights that consumers will enjoy from the CCPA.” \textit{Id.} at 109.\textsuperscript{169} See \textit{Is Artificial Intelligence a Threat to Privacy}, \textit{supra} note 83 (articulating the strength of the CCPA, and the potential for a similar federal legislation, which would mirror the EU’s GDPR).
be a clear set of guidelines which companies involved in data privacy issues would know to follow. Short of this proposed federal legislation, improvements in tort law would have a similar effect, as companies would be forced to take notice and make certain that their policies and products were not leaving them open to tort lawsuits for even unoffensive intrusions upon seclusion, eliminating the invasions of privacy in this other way. It seems unlikely that Citizen will address these concerns, which spread across all products that monitor users and collect user data, so either improved tort law, national data privacy legislation, or a combination of the two must be implemented to protect the privacy of consumers.